Indonesian Journal of Electrical Engineering and Computer Science
Vol. 14, No. 1, April 2019, pp. 353~359
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v14.i1.pp353-359

Testbed versus simulation approach on RF communication with AA_{β} asymmetric encryption scheme on internet of things devices

Syed Farid Syed Adnan, Mohd Anuar Mat Isa, Habibah Hashim
Information Security and Trusted Infrastructures Laboratory (InSTIL)
Faculty of Electrical Engineering, Universiti Teknologi MARAShah Alam, Selangor, Malaysia

Article Info

Article history:

Received Jun 19, 2018
Revised Sep 30, 2018
Accepted Dec 23, 2018

Keywords:

AA_{β}
Encryption
Internet of Things

ABSTRACT

The revolution of the Internet of Things (IoT) has given a better way of monitoring things including anything that could gather data and share the information over the internet. Most of the connected things are using Device to Device (D2D) connection to make it available on the internet such as client to a broker or client to a server. However, when IoT devices such as embedded devices and sensors that are connected to the internet, it becomes an open path for attackers to acquire the data and data vulnerably will become an issue. Thus, data integrity might become an issue, or the attackers could temper the data and could cause a disastrous domino effect to the interconnected IoT devices. Therefore, the data security collected from the sensors is substantial even though it could be a single character transmitted. However, IoT sensors are low powered devices in term of CPU, storage, memory and batteries. Securing the devices such as integrating theencryption algorithm computations might give overhead to the sensors and draining the batteries even faster than it is predicted.Alternatively, this paper attempts to explore the capabilities of the asymmetric scheme on resource constrained devices for its communications. Thus, this paper presents an RF communication analysis of a low consumption asymmetric encryption, the AAβ (AA-Beta) especially on encryption section that is likely to be feasible on IoT devices to preserve the data integrity.The design of RF transmission has been considered to suit the RF transceiver capability to prevent data losses and error from occurring. The result shows that 2.35 times of RF transmits runtime increased compared to RF simulation runtime. Meanwhile, at the receiver side, the runtime increases 60% compared to the simulation.

Corresponding Author:

Syed Farid Syed Adnan,
Information Security and Trusted Infrastructures Laboratory (InSTIL)
Faculty of Electrical Engineering
Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia.
Email: farrid85@gmail.com

1. INTRODUCTION

In the world of the Internet of Things (IoT), a lot of tasks has been made easier for our life.IoT enables interconnected of things equipped with embedded such as in vehicles, houses and even cities that allows the things autonomously share the data on the internet [1]. Bythe year 2025, 100 billion IoT devices connected is predictable[2]. Online real-time monitoring including smart home, smart city and even smart classroom hascreated a demand to make things easier. This lead to the autonomous world where all things are unified on the internet. For an example, current monitoring in an office building can be view on handheld devices for real-timeobservation. Any spike in current consumption can be detected with this features, where the additional waste of energy occurs can be monitored. Thus, it enables energy saving in an office environment. Another IoT application example by Ortiz et al.[3] that measure heart rates together with

waveforms. The data is then transmitted to the website and can be viewed instantly. Another example of IoT application by Subashini et al.[4] to monitor the crops humidity, temperature, light and soil moisture. The data are then transmitted to the server for analysis and database which can control the growth parameters.

However, IoT devices such as the current sensors, thedatais collected and exchanged openly on the internet. If security measures were not taken care of, unintentionally, this will open to adversariesthe likelihoods of data vulnerable. The adversaries could gain the data and tampered the data, that leads to data integrity issues.In 2015, Rose et al. [2] reported that IoT open to challenges such as security where IoT implementations will come upon new and unique security challenges. Some of the attack on thesensors including the replay attack, impersonation and compromise attacks [5]. Therefore, building up the trust for the devices by the users is crucial to prevent the data from being compromised [2]. Moreover, IoT framework security challenge including attacks at every layer gives an incrediblechallenge and new security requirements should be examined[6].

Internet of Things (IoT) Research study by Hewlett Packard (HP) [7] found out that 70 percent of IoT devices were running on unencrypted network services and 80 percent of the devices raised up privacy concerns. The research found out many devices neglected the encryption while updating the software updates and communication while connected to the internet is unencrypted. Meanwhile, the DHL logistics company reported in 2015 [8] that the automation by IoT technologymay lead to security vulnerabilities. Interconnection of IoT devices opens a path forcyber criminals could damage the IoT network for their own agenda. There fore, IoT security should be the priority especially the industry. In addition, an internet security report by Symantec in 2018, reported that 600% of IoT attacks increased in 2017 [9]. The attacks rather than paralyzing the interconnected network, the attackers choose to utilize the IoT resource to mining crypto coin.

On the network connection, the IoT devices need to get connected to share the data remotely. Wireless connection usually the main choice for device mobility instead of wired connection which has limited flexibility. The wireless technology ranging from Radio Frequency (RF), Bluetooth, WIFI and 3G or LTE connection [6][10]. However, the wireless technology chosen is based on the regulation, location, distance of the sensorsand energy consumption limitation for the things when connected to the network.An article by Mcadams [11] suggest RF communication possible to be the main player in the IoT environment as long as the right wireless designed for network reliability. Therefore, there are several researches on RF in IoT environment such as by Kanan et. al [12] in presented aresearch and tested in construction sites to prevent fatalities by utilizing RF at 868Mhz and IoT wearable device.Another work by Wang et. al [13]also proposed smart home control system with RF at 433Mhz and actuator network.

Securing the IoT devices including communication have been a highlight topic in IoT research.Li and Xiong [14] recommended a secured channel between the sensor node to the Internet resulting in reduced time and energy to the sensor nodes in the meantime security integrated. The author tested the scheme called heterogeneous signcryption on the online and offline application. Another research, Singh et al. [15]introduced *SPublish* that publishes encrypted data with lightweight ECC techniques through optimized parameters and computation algorithms. The authors designed and implemented the *SPublish* using secure MQTT protocols (SMQTT, SMQTTSN) with new secure publish command, the *SPublish*.In another research, Wang et al. [16]that implementedandroid based phone called Attribute-Based Encryption (ABE) with Java library utilizing the asymmetric encryption scheme. However, the works by Singh et al. [15] have shown better result,especially performance compared to Wang et al. [16]. One of the lists mentioned in [17], listed encryption as one of the key technology to improved IoT Security. Therefore, this research focusing on the communication between IoT devices including an asymmetric encryption scheme.

2. AA_β CRYPTOSYSTEM

A number of techniques have been developed to secure IoT things. The technique from previous research varies fromsymmetric to asymmetric encryption or even hybrid schemeis possible to secure IoT devices. Therefore, this motivates this study to explore the asymmetric encryption scheme, namely AA-Beta (AA_β) scheme competence on IoT environment.AA_β is anasymmetric crypto scheme that was introduced by Ariffin et al. in 2012 [18] utilizing the hardness of integer factorization problem. The authors demonstrated empirically that AA_βencryption shows faster runtime compare to other asymmetric encryption schemes, such as the Rivest Shamir Adleman (RSA) and Elliptic curve cryptography (ECC).

Moreover, on the decryption part, the performance was stated by Ariffin et. al [18] was as fast as RSA and marginally behind ECC. In another experiment demonstrated by Ariffin et al. [19], they have tested their scheme on Maple 13 using Windows 7 operating system and showed that AA_βencryption is capable with large data sets and large key size at faster runtime compared to RSA and ECC scheme. Generally, the AA_β

encryption scheme algorithm that discovered by Ariffin et al. in 2012 [18] can be represented with key generation, encryption and decryption as described below:

a. AA_β Key Generation

AA_β key generation procedure is presented as in Algorithm 1 below:

Algorithm 1: *Key Generation for AA_β*

1. **BEGIN**
2. *Choose random primes p and q with the size of n-bit until* $p \equiv 3(mod\ 4)$ *and* $q \equiv 3(mod\ 4)$.
3. *Get a random integer* $d > (p^2q)^{4/9}$
4. *Get integer e such that* $e.d \equiv 1\ mod\ pq$
- *Add multiple p.q until* $2^{3n+4} < e < 2^{3n+6}$ *(if necessary)*
5. *Get A1 =* p^2q *where* $2^{3n} < A_1 < 2^{3n+3}$
6. *Set A2 = e*
7. *Return* (n, A_1, A_2) *and* (pq, d)
8. **END**

b. AA_β Encryption

The AA_β encryption procedure can be defined in Algorithm 2:

Algorithm 2: AA_β Encryption

1. **BEGIN**
2. *Get plaintext M*
3. *Divide plaintext M to get plaintext pair* m_1 *and* m_2
4. *Compute ciphertext,* $C = A_1m_1 + A_2{m_2}^2$
5. *Return ciphertext, C*
6. **END**

c. AA_β Decryption

The AA_β decryption process is presented in Algorithm 3 below:

Algorithm 3: AA_β Decryption

1. **BEGIN**
2. *Read ciphertext, C*
3. Compute $\boldsymbol{W \equiv C\ (mod\ pq)}$
4. *Compute* $V_{i=1} \equiv x_pM_1q + (x_qM_2p)(mod\ pq)$
5. *Compute* $V_{i=2} \equiv x_pM_1q - (x_qM_2p)\ (mod\ pq)$
6. *Compute* $V_{i=3} \equiv -x_pM_1q + (x_qM_2p)\ (mod\ pq)$
7. *Compute* $V_{i=4} \equiv -x_pM_1q - (x_qM_2p)\ (mod\ pq)$
8. *Loop*

$$Compute\ m_{1_i} = \frac{C - Vi^2\ A_2}{A_1}$$

9. *While counter<4*
10. *If* $m_{1_i} > 0$, *pick the pair* (m_{1_i}, V_i)
11. *Set* $m_{2_i} = V_i$
12. *Return the plaintext* $M = 2^{4n}m_1 + m_2$
13. **END**

From the algorithm described above, the AA_β encryption schemegeneral ideacan beshown in Figure 1. The public key (n, A_1, A_2) are publicly available on the network for all devices. This can be visualized in form of Along and Busu, which are an example of two entities to establish secure communication. Along can be represented as the server, while Busu in this position is the Client.

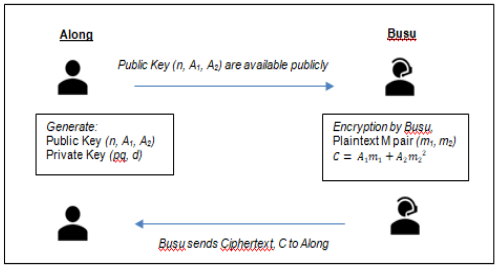

Figure 1. AA_β Encryption Process

Then,for the AA_βdecryption scheme, the process can be illustrated in Figure 2. The private *key (pq, d)* only available to the key owner, in this case, it is Along and the private key camdecryptsBusu's message.

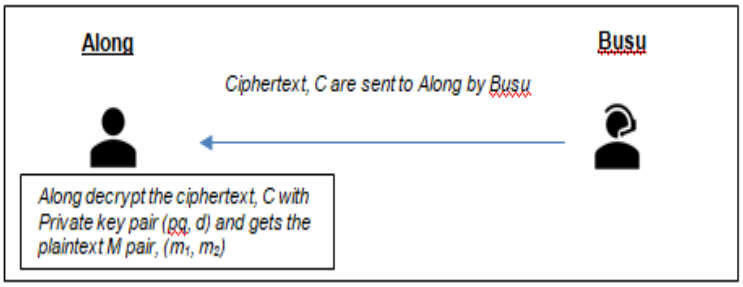

Figure 2. AA_βDecryption Process

3. EXPERIMENTAL SETUP

Generally, the experiments consist of encrypted data transmission using RF network. The setup consists of a client and a server that based on Raspberry Pi 3 device. Each of the devices is equipped with an RF transceiver. Meanwhile, for the environment used in this setup is the Raspbian Operating System (OS). The Raspbian OS is a Linux OS that has been enhanced for Raspberry Pi,embedded devices that are based on the ARM processor.The platform specification is:

a) Raspberry Pi 3, based on 4 x ARM Cortex-A53Quad Core 1.2GHz by Broadcomand 1Gb of RAM.This experiment running on Raspbian OS version called "Jessie".
b) For the RF module, the device is CisecoSlice of Radio Wireless RF Transceiver module paired with Raspberry Pi 3. The RF transceiver able to transmits and receive up to 200 meters in sight without an antenna attached.

The RF module is chosen in this experiment because of the lower energy required by the RF compared to WIFI technology. The design considers a testbed where the sensors are in sight in a room to transmits the payload.

Next, the codes were designed to work on the embedded device. For this experiment, the codes were written using the C programming language for AA_β encryption process on the Raspbian environment. To handle multiple precision numbers and optimize the encryption process, the codes were written with Bignum library (GMP). GMP library is usually used for arbitrary precision arithmetic that supports the calculations up to the available memory of the system rather than having a limitation on the types of the variable itself [20].

Meanwhile, for the communications between devices with RF, the codes are written in Python scripting. The communications included transmission (Tx) and receive (Rx) while the transmission speed chosen is 115200 baud rate. The RF frequency used in this experiment is 868Mhz. For the size of plaintext pair, m_1 and $m_2$selected in this experiment are based on the condition below where:

a) $2^{4n} < m_1 < 2^{4n+1}$
b) $2^{2n-2} < m_2 < 2^{2n-1}$

Where *n* is the length of prime and *m* is the plaintext. The plaintext range used is based on Ariffin et al. definition in [18]. Meanwhile, this research assumed the key generation is generated earlier and the public key ispreshared with the client and the server.

4. RESULTS AND ANALYSIS

This section presents the results of the experiment setup from the previous section.The results include the RF simulation transmission and receive runtime while transmitting the data.

Table 1 shows the RF simulation for AA_βon Raspberry Pi 2 platform from our previous research [21]. The data size is referring to the ciphertext generated from the encryption section. In this experiment, the data size is represented in bits. Table 1 shows the results simulatedwith serial communication simulated a client transmitting data to the server. This could be a transmission from a sensor to a server, where low runtime and low energy is required especially for aresource-constraineddevice.

Table 1.Raspberry Pi 2 AA_{β}RF Transmission Simulation Runtime [21]

Key Size	Data Size (bits)	Encryption (s)	Decryption (s)	Client Transmits(s)	Server Received(s)
1536	3587	0.0009587	0.0186161	0.001234667	0.056090333
3072	7172	0.001755	0.1153961	0.001349667	0.120447333
6144	14340	0.0039217	0.7234373	0.001716667	0.239137333

Next, this research continues the experiment with Raspberry Pi 3 transmission, this time with real working RF transmission.Table *2*below shows the RF transmission runtime with RF on Raspberry Pi 3.

Table 2. Raspberry Pi 3 AA_{β} RF Transmission Runtime

Key Size	Data Size (bits)	Client Transmits(s)	Server Received(s)
1536	3587	0.0014275	0.073496
3072	7172	0.0021795	0.19384
6144	14340	0.0041542	0.3934999

Figure 3 shows the comparison of AA_{β}RF simulation with the real working RF transmission total runtime.For the key size of 6144- bit, the RF transmits runtime increase aroundtwo-fold compared to RF transmits during simulation runtime. Meanwhile, server received runtime increased 60% compared to RF simulation. This is due to several delays added to the designed of RF transmission on Python programming. The delays added to the RF transceiver to control the buffer from being full while transmitting the ciphertext that could cause data losses. With simulation, there are no losses occur, resulting in faster transmits and received runtime.

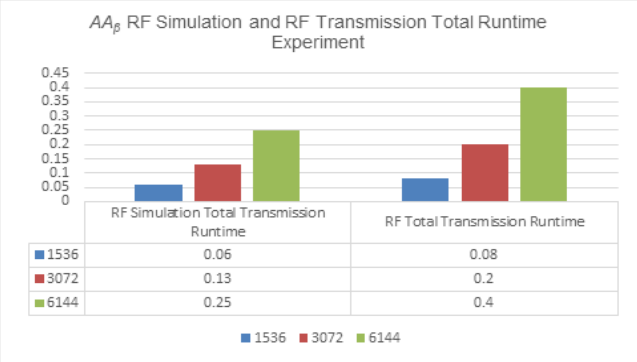

Figure 3. AA_{β} RF Simulation and RF Transmission Total Runtime

Given the scenario above, the measured current on Raspberry Pi 2 is 0.258A at 5 Volt and Raspberry Pi 3 current at 0.279A at 4.86V. Table 3 shows the RF transmits runtime along with runtime current, voltage, power andenergy consumed during transmission of AA_{β}ciphertext. Meanwhile, Table 4. shows the runtime energy consumed at the receiver side. The designed RF communications at receiver side required longer runtime and energy compared to transmits runtime and energy. This happens because of receiver delay added longer than transmits delay. The RF added longer delay receiving the data correctly to avoid the buffer being full, limited by the RF device. If the transmission is not being controlled, the received data will be mixed up while more data incoming at receiver and resulting in wrong data acquired.

Table 3.AA_{β}RF Transmits Runtime Experiment

Key Size	Data Size (Byte)	RF Runtime (s)	Runtime Current (A)	Runtime Voltage (V)	Power (Watt)	Energy (Joules)
1536	600	0.0014275	0.279	4.86	1.356	0.001936
3072	1196	0.0021795	0.279	4.86	1.356	0.002955
6144	2392	0.0041542	0.279	4.86	1.356	0.005633

Table 4. AA_{β}RF Receive Runtime Experiment

Key Size	Data Size (Byte)	RF Runtime (s)	Current Runtime (A)	Voltage Runtime (V)	Power (Watt)	Energy (Joules)
1536	600	0.073496	0.279	4.86	1.395	0.099656
3072	1196	0.19384	0.279	4.86	1.395	0.262835
6144	2392	0.3934999	0.279	4.86	1.395	0.533562

Figure 4 illustrated the energy required in Joules for RF transmits and received respectively. When key size and plaintext increased, the longer time is taken for receiving resulting higher energy consumed. Meanwhile, the energy for transmits is almost equal for all key size. This can be concluded that it is feasible for energy constrained devices, especially for data encryption and transmission. Meanwhile, the longer time taken for received willadd higher energy overhead for the resource-constrained device. This is suitable for a condition where the data collected from the sensors and processed at the centralized processing such as the server.

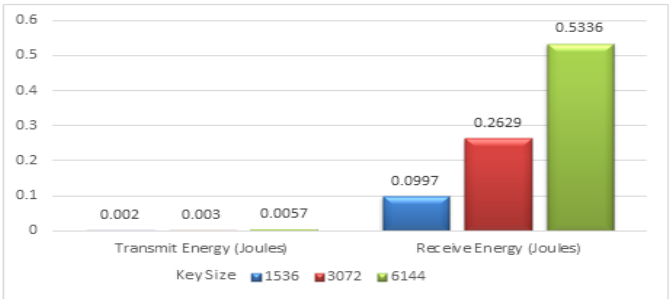

Figure 4. AA_{β} RF Transmits and Receive Energy

Hence, in RF simulation, the encryption and transmission process with a key size of 6144-bit, the time taken is 0.968 seconds. Therefore, the calculated total energy is 1.249 Joules per session.Meanwhile, for the real experiment of RF transmission, the total time taken calculated is 1.125 seconds at 1.525 Joules per session. An increase of 57.54% from the simulation to the real RF experiment can be seen for the key size of 6144-bitcaused by the extra delay added to control the communication.

5. CONCLUSION

This research introduced an asymmetric encryption scheme, the AA_{β} encryption scheme together with RF transmission testbed to test the Internet of Things encrypted communications. This research also compared with the simulated results from the previous publication. The results showthe AA_{β}testbed setup with RF transceiver getting an increase of runtime and energy compared to the simulation. For the transmit side, the runtime increased two-fold for the largest key size and payload size. On the other hand, the receiver runtime increased 60% from the simulation. The transmission for both simulation and the working testbed was designed with the same Python scripting, baud rate and payload size for each key size. However, controlling the real RF transmission requiresa differen tapproach to avoid any error in transmission over the RF connection. The difference between simulation and working RF transmission, there is no error or scrambled payload received at the receiver during simulationeven up for 200 times data transmission where advised by Putra et al. [22] in transmitting the data in the wireless network. The RF transmits might be beneficial to multi-sensor device while encrypting the payload with AA_{β} where the low energy required to encrypt and transmits the payload.Even though the payload size is getting bigger and higher key size required, the runtime and energy required almost evenly across all key size tested in this research.The future work can be extended to another wireless technology such as WIFI or Bluetooth network for better result compared to RF received section with Message Queuing Telemetry Transport (MQTT) protocol might be useful for the resource-constrained device.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the Ministry of Higher Education (MOHE) Malaysia for providing the grant 600-RMI/NRGS 5/3 (5/2013) and Universiti Teknologi MARA (UiTM) for supporting this research work.

REFERENCES

[1] Margaret Rouse and Ivy Wigmore, *"Internet of Things (IoT),"* *Tech Target*. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed: 29-Feb-2016].
[2] K. Rose, S. Eldridge, and C. Lyman, "*The internet of things: an overview*," *Internet Soc.*, no. October, p. 53, 2015.
[3] K. J. P. Ortiz, J. P. O. Davalos, E. S. Eusebio, and D. M. Tucay, "*IoT: Electrocardiogram (ECG) monitoring system*," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 2, pp. 480–489, 2018.
[4] M. S. M, S. Das, S. Heble, U. Raj, and R. Karthik, "*Internet of Things based Wireless Plant Sensor for Smart Farming*," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 2, pp. 456–468, 2018.
[5] K. N. Q. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, "*Security in Wireless Sensor Network : Approaches and Issues*," *TELKOMNIKA Indones. J. Electr. Eng.*, vol. 15, no. 3, pp. 584–590, 2015.
[6] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "*Internet of things (IoT) security: Current status, challenges and prospective measures*," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. pp. 336–341, 2015.
[7] Hewlett Packard Enterprise, "*Internet of Things Research Study 2015 Report*," no. July, p. 4, 2015.
[8] J. Macaulay, L. Buckalew, and G. Chung, "Internet of Things in Logistics," *DHL Trend Res.*, vol. 1, no. 1, pp. 1–27, 2015.
[9] Symantec, "*2018 Internet Security Threat Report*," 2018.
[10] F. K. Santoso and N. C. H. Vun, "*Securing IoT for smart home system*," *Proc. Int. Symp. Consum. Electron. ISCE*, vol. 2015–Augus, pp. 5–6, 2015.
[11] B. Mcadams, "*RF FUNDAMENTALS for the INTERNET of THINGS*," 2017. [Online]. Available: https://oleumtech.com/wp-content/uploads/downloads/references/rf-fundamentals-for-iot-iiot-oleumtech.pdf.
[12] R. Kanan, O. Elhassan, and R. Bensalem, "*An IoT-based autonomous system for workers' safety in construction sites with real-time alarming, monitoring, and positioning strategies*," *Autom. Constr.*, vol. 88, no. November 2016, pp. 73–86, 2018.
[13] M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, "*An IoT-based appliance control system for smart homes*," in *Proceedings of the 2013 International Conference on Intelligent Control and Information Processing, ICICIP 2013*, 2013, pp. 744–747.
[14] F. Li and P. Xiong, "*Practical secure communication for integrating wireless sensor networks into the internet of things*," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3677–3684, 2013.
[15] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "*Secure MQTT for Internet of Things (IoT),*" *Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015*, pp. 746–751, 2015.
[16] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "*Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT*," *2014 IEEE Int. Conf. Commun. ICC 2014*, pp. 725–730, 2014.
[17] J. Blyler, "*8 Critical IoT Security Technologies*," in *Electronic Design*, 2017.
[18] M. R. K. Ariffin, M. A. Asbullah, N. A. Abu, and Z. Mahad, "*A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of N=P^2 .q*," *Malaysian J. Math. Sci. 7(S) 19-37 Spec. Issue 3rd Int. Conf. Cryptol. Comput. Secur. 2012*, vol. 7, pp. 1–6, 2012.
[19] Z. Mahad and M. R. K. Ariffin, *"AABeta public key cryptosystem - A new practical asymmetric implementation based on the square root problem*," in *Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*, 2012, pp. 584–588.
[20] The GNU MP Bignum Library, "*The GNU Multiple Precision Arithmetic Library (GMP) Library*." [Online]. Available: https://gmplib.org/. [Accessed: 25-Mar-2016].
[21] S. F. S. Adnan, M. A. M. Isa, and H. Hashim, "*RF simulations for AAβ cryptosystem, an asymmetric encryption scheme*," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 2, pp. 542–548, 2018.
[22] G. D. Putra, A. R. Pratama, A. Lazovik, and M. Aiello, "C*omparison of energy consumption in Wi-Fi and bluetooth communication in a Smart Building*," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–6.